

# COUNTING INVERTIBLE SUMS OF SQUARES MODULO $n$ AND A NEW GENERALIZATION OF EULER TOTIENT FUNCTION

CATALINA CALDERÓN, JOSÉ MARÍA GRAU, AND ANTONIO M. OLLER-MARCÉN

**ABSTRACT.** In this paper we introduce and study a family  $\Phi_k$  of arithmetic functions generalizing Euler's totient function. These functions are given by the number of solutions to the equation  $\gcd(x_1^2 + \cdots + x_k^2, n) = 1$  with  $x_i \in \mathbb{Z}/n\mathbb{Z}$  which, for  $k = 2, 4$  and  $8$  coincide, respectively, with the number of units in the rings of Gaussian integers, quaternions and octonions over  $\mathbb{Z}/n\mathbb{Z}$ . We prove that  $\Phi_k$  is multiplicative for every  $k$ , we obtain an explicit formula for  $\Phi_k(n)$  in terms of the prime-power decomposition of  $n$  and we study some properties that extend well-known results for  $\varphi$ . As a tool we study the multiplicative arithmetic function that counts the number of solutions to  $x_1^2 + \cdots + x_k^2 \equiv \lambda \pmod{n}$  for  $\lambda$  coprime to  $n$ , thus extending an old result that dealt only with the prime  $n$  case.

## 1. INTRODUCTION

Euler's totient function  $\varphi$  is one of the most famous arithmetic functions used in number theory. Recall that  $\varphi(n)$  is defined as the number of positive integers less than or equal to  $n$  that are coprime to  $n$ . Many generalizations Euler's function are known. See, for instance [4, 6, 7, 11, 14] or the special chapter on this topic in [13]. Among these generalizations, the most significant is probably the so-called Jordan's totient function [1, 2, 16] defined as  $\mathbf{J}_k(n) := n^k \prod_{p|n} (1 - p^{-k})$ . In this paper we introduce and study a new generalization of  $\varphi$ . In particular, given  $k \in \mathbb{N}$  we define

$$\Phi_k(n) := \text{card} \{(x_1, \dots, x_k) \in \mathbb{Z}^k : 0 \leq x_i < n \text{ and } \gcd(x_1^2 + \cdots + x_k^2, n) = 1\}.$$

Clearly  $\Phi_1(n) = \varphi(n)$  and it is the order of the group of units of the ring  $\mathbb{Z}/n\mathbb{Z}$ . On the other hand,  $\Phi_2(n)$  is the so-called GIphi which computes the number of Gaussian integers in a reduced system modulo  $n$ . In the same way,  $\Phi_4(n)$  and  $\Phi_8(n)$  compute, respectively, the number of invertible quaternions and octonions over  $\mathbb{Z}/n\mathbb{Z}$ .

In order to study the function  $\Phi_k$  we need to focus on the functions

$$\rho_{k,\lambda}(n) := \text{card} \{(x_i, \dots, x_k) \in (\mathbb{Z}/n\mathbb{Z})^k : x_1^2 + \cdots + x_k^2 \equiv \lambda \pmod{n}\}$$

which count the number of points on hyperspheres in  $(\mathbb{Z}/n\mathbb{Z})^k$  and, in particular, in the case  $\gcd(\lambda, n) = 1$ . These functions were already studied in the case when  $n$  is an odd prime by V.H. Lebesgue in 1837. In particular he proved the following result [3, Chapter X].

**Proposition 1.** *Let  $p$  be an odd prime and let  $k, \lambda$  be positive integers with  $p \nmid \lambda$ . Put  $t = (-1)^{(p-1)(k-1)/4} p^{(k-1)/2}$  and  $l = (-1)^{k(p-1)/4} p^{(k-2)/2}$ . Then,*

$$\rho_{k,\lambda}(p) = \begin{cases} p^{k-1} + t, & \text{If } k \text{ is odd and } \lambda \text{ is a quadratic residue modulo } p; \\ p^{k-1} - t, & \text{If } k \text{ is odd and } \lambda \text{ is a not quadratic residue modulo } p; \\ p^{k-1} - l, & \text{If } k \text{ is even.} \end{cases}$$

The paper is organized as follows. First of all, in Section 2 we study the values of  $\rho_{k,\lambda}(n)$  in the case  $\gcd(\lambda, n) = 1$ , thus generalizing Lebesgue's work. In Section 3 we study the functions  $\Phi_k$ , in particular we prove that they are multiplicative and we give a closed formula for  $\Phi_k(n)$  in terms of the prime-power decomposition of  $n$ . Finally, we close our work presenting some properties of the functions  $\Phi_k$  that generalize known properties of Euler's totient function (which are recovered if  $k = 1$ ) and suggesting some ideas that leave the door open for future work.

## 2. COUNTING POINTS ON HYPERSPHERES (mod $n$ )

Due to the Chinese Remainder Theorem, the function  $\rho_{k,\lambda}$  is multiplicative; i.e., if  $n = p_1^{r_1} \cdots p_m^{r_m}$ , then  $\rho_{k,\lambda}(n) = \rho_{k,\lambda}(p_1^{r_1}) \cdots \rho_{k,\lambda}(p_m^{r_m})$ . Hence, we can restrict ourselves to the case when  $n = p^s$  is a prime-power. Moreover, since in this paper we focus on the case  $\gcd(\lambda, n) = 1$ , we will always assume that  $p \nmid \lambda$ . The following result will allow us to extend Lebesgue's work to the odd prime-power case.

**Lemma 1.** *Let  $p$  be an odd prime and let  $s \geq 1$ . If  $p \nmid \lambda$ , then*

$$\rho_{k,\lambda}(p^s) = p^{(s-1)(k-1)} \rho_{k,\lambda}(p).$$

*Proof.* It is easily seen that any solution to the congruence  $x_1^2 + \cdots + x_k^2 \equiv \lambda \pmod{p^{s+1}}$  must be of the form  $(a_1 + t_1 p^s, \dots, a_k + t_k p^s)$  for some  $(a_1, \dots, a_k)$  such that  $a_1^2 + \cdots + a_k^2 \equiv \lambda \pmod{p^s}$ . Now,  $(a_1 + t_1 p^s)^2 + \cdots + (a_k + t_k p^s)^2 \equiv \lambda \pmod{p^{s+1}}$  if and only if  $2a_1 t_1 + \cdots + 2a_k t_k \equiv -K \pmod{p}$ , where  $K$  is such that  $a_1^2 + \cdots + a_k^2 = Kp^s + \lambda$ . Since  $a_i \not\equiv 0 \pmod{p}$  for some  $i \in \{1, \dots, k\}$ , it follows that there are exactly  $p^{k-1}$  possibilities for  $(t_1, \dots, t_k)$  and the result follows inductively.  $\square$

If  $p = 2$  we have a similar result.

**Lemma 2.** *Let  $s \geq 3$  and let  $\lambda \geq 1$  be odd. Then,*

$$\rho_{k,\lambda}(2^s) = 2^{(s-3)(k-1)} \rho_{k,\lambda}(8).$$

*Proof.* If  $s \geq 3$  it can be easily seen that any solution to the congruence  $x_1^2 + \cdots + x_k^2 \equiv \lambda \pmod{2^{s+1}}$  must be of the form  $(a_1 + t_1 2^{s-1}, \dots, a_k + t_k 2^{s-1})$  for some  $(a_1, \dots, a_k)$  such that  $a_1^2 + \cdots + a_k^2 \equiv \lambda \pmod{2^s}$ . Now,  $(a_1 + t_1 2^{s-1})^2 + \cdots + (a_k + t_k 2^{s-1})^2 \equiv \lambda \pmod{2^{s+1}}$  if and only if  $a_1 t_1 + \cdots + a_k t_k \equiv -K \pmod{2}$ , where  $K$  is such that  $a_1^2 + \cdots + a_k^2 = K2^s + \lambda$ . Since  $a_i$  must be odd for some  $i \in \{1, \dots, k\}$ , it follows that there are exactly  $2^{k-1}$  possibilities for  $(t_1, \dots, t_k)$  and the result follows inductively.  $\square$

As we have just seen, unlike when  $p$  is an odd prime, the recurrence is now based on  $\rho_{k,\lambda}(2^3)$ . Hence, the cases  $s = 1, 2, 3$ ; i.e.,  $n = 2, 4, 8$ , must be studied separately. In order to do so, the following general result will be useful.

**Proposition 2.** *Let  $k, \lambda \geq 1$  and let  $n$  be a positive integer. Then,*

$$\rho_{k,\lambda}(n) = \sum_{i=0}^{n-1} \rho_{1,i}(n) \rho_{k-1,\lambda-i}(n).$$

*Proof.* Let  $(x_1, \dots, x_k) \in A(k, \lambda, n)$ ; i.e.,  $x_1^2 + \dots + x_k^2 \equiv \lambda \pmod{n}$ . Then, for some  $i \in \{0, \dots, n-1\}$  we have that  $x_1^2 \equiv i \pmod{n}$  and  $x_2^2 + \dots + x_k^2 \equiv \lambda - i \pmod{n}$  and hence the result.  $\square$

Now, given  $k, n \geq 1$  let us define the matrix  $M(n) = \left( \rho_{1,i-j}(n) \right)_{0 \leq i,j \leq n-1}$ . If we consider the column vector  $R_k(n) = \left( \rho_{k,i}(n) \right)_{0 \leq i \leq n-1}$ , then Lemma 2 leads to the following recurrence relation:

$$R_k(n) = M(n) \cdot R_{k-1}(n).$$

In the following proposition we use this recurrence relation to compute  $\rho_{k,\lambda}(2^s)$  for  $s = 1, 2, 3$  and odd  $\lambda$ .

**Proposition 3.** *Let  $k$  be a positive integer. Then:*

- i)  $\rho_{k,1}(2) = 2^{k-1}$ ,
- ii)  $\rho_{k,1}(4) = 4^{k-1} + 2^{\frac{3k}{2}-1} \sin\left(\frac{\pi k}{4}\right)$ ,
- iii)  $\rho_{k,3}(4) = 4^{k-1} - 2^{\frac{3k}{2}-1} \sin\left(\frac{\pi k}{4}\right)$ ,
- iv)  $\rho_{k,1}(8) = 2^{2k-3} \left( 2^k + 2^{\frac{k}{2}+1} \sin\left(\frac{\pi k}{4}\right) + 2 \sin\left(\frac{1}{4}\pi(k+1)\right) - 2 \cos\left(\frac{1}{4}(3\pi k + \pi)\right) \right)$ ,
- v)  $\rho_{k,3}(8) = 2^{2k-3} \left( 2^k - 2^{\frac{k}{2}+1} \sin\left(\frac{\pi k}{4}\right) - 2 \left( \cos\left(\frac{1}{4}\pi(k+1)\right) + \cos\left(\frac{3}{4}\pi(k+1)\right) \right) \right)$ ,
- vi)  $\rho_{k,5}(8) = 2^{2k-3} \left( 2^k + 2^{\frac{k}{2}+1} \sin\left(\frac{\pi k}{4}\right) - 2 \sin\left(\frac{1}{4}\pi(k+1)\right) + 2 \cos\left(\frac{1}{4}(3\pi k + \pi)\right) \right)$ ,
- vii)  $\rho_{k,7}(8) = 2^{2k-3} \left( 2^k - 2^{\frac{k}{2}+1} \sin\left(\frac{\pi k}{4}\right) - 2 \sin\left(\frac{1}{4}(3\pi k + \pi)\right) + 2 \cos\left(\frac{1}{4}\pi(k+1)\right) \right)$ .

*Proof.* First of all, observe that

$$M(2) = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \quad M(4) = \begin{pmatrix} 2 & 0 & 0 & 2 \\ 2 & 2 & 0 & 0 \\ 0 & 2 & 2 & 0 \\ 0 & 0 & 2 & 2 \end{pmatrix}, \quad M(8) = \begin{pmatrix} 2 & 0 & 0 & 0 & 2 & 0 & 0 & 4 \\ 4 & 2 & 0 & 0 & 0 & 2 & 0 & 0 \\ 0 & 4 & 2 & 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 4 & 2 & 0 & 0 & 0 & 2 \\ 2 & 0 & 0 & 4 & 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 4 & 2 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 4 & 2 & 0 \\ 0 & 0 & 0 & 2 & 0 & 0 & 4 & 2 \end{pmatrix}.$$

Let us compute ii). We know that  $R_k(4) = M(4) \cdot R_{k-1}(4)$ . Hence, since the eigenvalues of  $M(4)$  are  $\{4, 2+2i, 2-2i, 0\}$ , we know that

$$\rho_{k,1}(4) = C_1 4^k + C_2 (2+2i)^k + C_3 (2-2i)^k.$$

In order to compute  $C_1$ ,  $C_2$  and  $C_3$  it is enough to observe that  $\rho_{1,1}(4) = 2$ ,  $\rho_{2,1}(4) = 8$  and  $\rho_{3,1}(4) = 24$ . Hence:

$$\begin{aligned} 4C_1 + (2+2i)C_2 + (2-2i)C_3 &= 2, \\ 16C_1 + 8iC_2 - 8iC_3 &= 8, \\ 64C_1 - (16-16i)C_2 - (16+16i)C_3 &= 24. \end{aligned}$$

And we get

$$\rho_{k,1}(4) = \frac{1}{4} (4^k - i(2+2i)^k + i(2-2i)^k) = 2^{2k-2} + 2^{\frac{3k}{2}-1} \sin\left(\frac{\pi k}{4}\right),$$

as claimed.

To compute the other cases note that the eigenvalues of  $M(2)$  are  $\{0, 2\}$  while the eigenvalues of  $M(8)$  are

$$\left\{8, 4+4i, 4-4i, \sqrt{2}(-2-2i), \sqrt{2}(2+2i), \sqrt{2}(-2+2i), \sqrt{2}(2-2i), 0\right\}.$$

Thus, in each case we only need to compute the corresponding initial conditions and constants. The final results have been obtained with the help of Mathematica “ComplexExpand” command.  $\square$

### 3. COUNTING INVERTIBLE SUMS OF SQUARES MODULO $n$

Given positive integers  $k, n$ , this section is devoted to computing the number of solutions of  $\gcd(x_1^2 + \cdots + x_k^2, n) = 1$ , that we shall denote by  $\Phi_k(n)$ . First of all, let us define the set

$$\mathcal{A}_k(n) := \bigcup_{\substack{1 \leq \lambda \leq n \\ \gcd(\lambda, n)=1}} A(k, \lambda, n).$$

Hence,  $\Phi_k(n) = \text{card } \mathcal{A}_k(n)$  and, since the union is clearly disjoint, it follows that

$$\Phi_k(n) = \sum_{\substack{1 \leq \lambda \leq n \\ \gcd(\lambda, n)=1}} \rho_{k,\lambda}(n).$$

The following result shows the multiplicativity of  $\Phi_k$  for every positive  $k$ .

**Theorem 1.** *Let  $k$  be a positive integer. Then  $\Phi_k$  is multiplicative; i.e.,  $\Phi_k(mn) = \Phi_k(m)\Phi_k(n)$  for every  $m, n \in \mathbb{Z}$  such that  $\gcd(m, n) = 1$ .*

*Proof.* Let us define a map  $F : \mathcal{A}_k(m) \times \mathcal{A}_k(n) \longrightarrow \mathcal{A}_k(mn)$  by

$$F((a_1, \dots, a_k), (b_1, \dots, b_k)) = (na_1 + mb_1, \dots, na_k + mb_k).$$

Note that if  $(a_1, \dots, a_k) \in \mathcal{A}_k(m)$ , then  $a_1^2 + \cdots + a_k^2 \equiv \lambda_1 \pmod{m}$  for some  $\lambda_1$  with  $\gcd(\lambda_1, m) = 1$ . In the same way, if  $(b_1, \dots, b_k) \in \mathcal{A}_k(n)$ , then  $b_1^2 + \cdots + b_k^2 \equiv \lambda_2 \pmod{n}$  for some  $\lambda_2$  with  $\gcd(\lambda_2, n) = 1$ . Consequently,

$$\begin{aligned} (na_1 + mb_1)^2 + \cdots + (na_k + mb_k)^2 &= n^2(a_1^2 + \cdots + a_k^2) + m^2(b_1^2 + \cdots + b_k^2) \\ &\quad + 2mn(b_1a_1 + \cdots + b_ka_k) \equiv \\ &\equiv n^2\lambda_1 + m^2\lambda_2 \pmod{mn}. \end{aligned}$$

Since it is clear that  $\gcd(n^2\lambda_1 + m^2\lambda_2, mn) = 1$ , it follows that  $(na_1 + mb_1, \dots, na_k + mb_k) \in \mathcal{A}_k(mn)$  and thus  $F$  is well-defined.

Now, let  $(c_1, \dots, c_k) \in \mathcal{A}_k(mn)$ . Then  $c_1^2 + \cdots + c_k^2 \equiv \lambda \pmod{mn}$  for some  $\lambda$  such that  $\gcd(\lambda, mn) = 1$ . Let us define  $a_i \equiv c_i \pmod{m}$  and  $b_i \equiv c_i \pmod{n}$  for every  $i = 1, \dots, k$ . It follows that  $(a_1, \dots, a_k) \in \mathcal{A}_k(m)$ ,  $(b_1, \dots, b_k) \in \mathcal{A}_k(n)$  and, moreover,  $F((a_1, \dots, a_k), (b_1, \dots, b_k)) = (c_1, \dots, c_k)$ . Hence,  $F$  is surjective.

Finally, assume that

$$(na_1 + mb_1, \dots, na_k + mb_k) \equiv (n\alpha_1 + m\beta_1, \dots, n\alpha_k + m\beta_k) \pmod{mn}$$

for some  $(a_1, \dots, a_k), (\alpha_1, \dots, \alpha_k) \in \mathcal{A}_k(m)$  and for some  $(b_1, \dots, b_k), (\beta_1, \dots, \beta_k) \in \mathcal{A}_k(n)$ . Then, for every  $i = 1, \dots, k$  we have that  $na_i + mb_i \equiv n\alpha_i + m\beta_i \pmod{mn}$ . From this, it follows that  $a_i \equiv \alpha_i \pmod{m}$  and that  $b_i \equiv \beta_i \pmod{n}$  for every  $i$  and hence  $F$  is injective.

Thus, we have proved that  $F$  is bijective and the result follows.  $\square$

Since we know that  $\Phi_k$  is multiplicative, we just need to compute its values over prime-powers. We do so in the following result.

**Proposition 4.** *Let  $k, r$  be positive integers. Then:*

- i)  $\Phi_k(2^r) = \varphi(2^{kr})$ .
- ii) *If  $p$  is an odd prime,*

$$\Phi_k(p^r) = \begin{cases} \varphi(p^{kr}), & \text{if } k \text{ is odd;} \\ \varphi(p^{kr}) - \varphi(p^{kr-k/2}), & \text{if } k \text{ is even and } 4 \mid k \text{ or } 4 \mid p-1; \\ \varphi(p^{kr}) + \varphi(p^{kr-k/2}), & \text{if } k \text{ is even, } 4 \nmid k \text{ and } 4 \nmid p-1. \end{cases}$$

*Proof.*

- i) If  $r = 1, 2, 3$  the result readily follows from Proposition 3 by simple computation. Now, if  $r > 3$  we can apply Lemma 2 to obtain that

$$\begin{aligned} \Phi_k(2^r) &= \sum_{\substack{1 \leq i \leq 2^r \\ 2 \nmid i}} \rho_{k,i}(2^r) = 2^{(r-3)(k-1)} \sum_{\substack{1 \leq i \leq 2^r \\ 2 \nmid i}} \rho_{k,i}(8) \\ &= 2^{(r-3)(k-1)} \sum_{j=0}^{2^{r-3}-1} \sum_{\substack{8j+1 \leq i \leq 8(j+1)-1 \\ 2 \nmid i}} \rho_{k,i}(8) = \\ &= 2^{(r-3)(k-1)} 2^{r-3} \sum_{\substack{1 \leq i \leq 7 \\ 2 \nmid i}} \rho_{k,i}(8) = \\ &= 2^{(r-3)(k-1)} 2^{r-3} 2^{3k-1} = 2^{rk-1} = \varphi(2^{kr}). \end{aligned}$$

- ii) Due to Lemma 1 it can be seen, as is the previous case, that

$$\Phi_k(p^r) = p^{k(r-1)} \sum_{i=1}^{p-1} \rho_{k,i}(p).$$

Thus, it is enough to apply Proposition 1.  $\square$

Finally, we summarize the previous work in the following result.

**Corollary 1.** *Let  $k, n$  be positive integers. Then,*

$$\Phi_k(n) = \begin{cases} n^{k-1} \varphi(n), & \text{if } k \text{ is odd;} \\ n^{k-1} \varphi(n) \prod_{2 \nmid p \mid n} \left(1 - \frac{1}{p^{k/2}}\right), & \text{if } k \equiv 2 \pmod{4}; \\ n^{k-1} \varphi(n) \prod_{\substack{p \mid n \\ p \equiv 3 \pmod{4}}} \left(1 + \frac{1}{p^{k/2}}\right) \prod_{\substack{p \mid n \\ p \equiv 1 \pmod{4}}} \left(1 - \frac{1}{p^{k/2}}\right), & \text{if } 4 \mid k. \end{cases}$$

*Proof.* Just apply the multiplicativity of  $\Phi_k$  and observe that

$$\begin{aligned}\varphi(p^{kr}) - \varphi(p^{kr-k/2}) &= p^{kr-\frac{k}{2}-1}(p-1)(p^{k/2}-1), \\ \varphi(p^{kr}) + \varphi(p^{kr-k/2}) &= p^{kr-\frac{k}{2}-1}(p-1)(p^{k/2}+1).\end{aligned}$$

□

When  $k$  is a multiple of 4,  $\Phi_k$  is closely related to  $\mathbf{J}_{k/2}$ . The following result makes this relation explicit. Its proof, that we omit, follows from the previous corollary recalling the definition of Jordan's totient function  $\mathbf{J}_k$ .

**Proposition 5.** *Let  $k$  be a multiple of 4. Then,*

$$\Phi_k(n) = n^{\frac{k}{2}-1} \mathbf{J}_{k/2}(n) \varphi(n) \frac{2^{\frac{k}{2}} - 1 - \text{mod}(n, 2)}{2^{\frac{k}{2}}}.$$

Moreover, if  $k/4$  is odd, we have that

$$\frac{\Phi_k(n)}{\Phi_{k/4}(n)} = n \mathbf{J}_{k/2}(n) \frac{2^{k/4} - 1 - \text{mod}(n, 2)}{2^{k/4}}$$

If  $k = 4$  recall that  $\Phi_4(n)$  is the number of units in the ring  $\mathbb{H}(\mathbb{Z}/n\mathbb{Z})$ . If, in addition,  $n$  is odd then  $\Phi_4(n) = n \mathbf{J}_2(n) \varphi(n)$  which is the well-known formula for the number of regular matrices in the ring  $M_2(\mathbb{Z}/n\mathbb{Z})$ . Of course, this is not a surprise since it is known that for an odd  $n$  the rings  $\mathbb{H}(\mathbb{Z}/n\mathbb{Z})$  and  $M_2(\mathbb{Z}/n\mathbb{Z})$  are isomorphic [5].

#### 4. SOME PROPERTIES OF $\Phi_k$

In this section we will present some properties of the function  $\Phi_k$  which are counterparts of known properties of Euler's totient function (recall that  $\Phi_1 = \varphi$ ).

##### 4.1. The first elementary properties of $\Phi_k$ .

**Proposition 6.** *Let  $m, n$  be positive integers such that  $n \mid m$ . Then,  $\Phi_k(n) \mid \Phi_k(m)$  for every  $k \geq 1$ .*

*Proof.* Note that, if  $p$  is prime and  $r \leq s$ , Proposition 4 implies that  $\Phi_k(p^r) \mid \Phi_k(p^s)$ . Hence, the result follows because  $\Phi_k$  is multiplicative. □

The function  $\Phi_k$  is multiplicative, but not completely multiplicative. The following result makes this clear.

**Proposition 7.** *Let  $m, n, k$  be positive integers and let  $d = \gcd(m, n)$ . Then,*

$$\Phi_k(mn) = \Phi_k(m) \Phi_k(n) \frac{d^k}{\Phi_k(d)}.$$

*Proof.* Let  $p$  be a prime and let  $r_1, r_2$  be positive integers with  $r_1 < r_2$ . If we put  $r = r_1 + r_2$ , Proposition 4 leads to

$$\Phi_k(p^r) = \Phi_k(p^{r_1}) \Phi_k(p^{r_2}) \frac{p^{kr_1}}{\Phi_k(p^{r_1})}.$$

Thus, it is enough to consider the prime-power decomposition of  $m$  and  $n$  to complete the proof. □

Finally, if we apply Proposition 7 in the case  $m = n$  we get the following.

**Corollary 2.** *Let  $n, k$  be positive integers. Then,*

$$\Phi_k(n^m) = n^{km-k} \Phi_k(n).$$

**4.2. Asymptotic growth of  $\Phi_k$ .** We now focus on the asymptotic behavior of  $\Phi_k(n)/n^k$ ; i.e., on the average number of points in  $[1, n]^k$  such that its sum of squares is coprime to  $n$ . We see that this behavior is independent of  $k$  and, moreover, that it is the same as that of  $\varphi(n)/n$ . See [8] for results on the asymptotic growth of Euler  $\varphi$  function and its limits.

**Proposition 8.** *For every positive integer  $k$  we have that:*

$$\limsup \frac{\Phi_k(n)}{n^k} = 1,$$

$$\liminf \frac{\Phi_k(n)}{n^k} = 0.$$

*Proof.* It is enough to apply Corollary 1 together with the known results for  $\varphi(n)/n$ .  $\square$

**4.3. Divisor sum and Möbius inversion formula.** The following identity is well-known:

$$S(n) := \sum_{d|n} \varphi(n) = n.$$

It follows from the fact that  $S$  is multiplicative and  $S(p^r) = p^r$  for every prime-power  $p^r$ . In terms of Dirichlet's convolution this identity can be written as  $S = U * \varphi = N$ , where the functions  $U$  and  $N$  are given by  $U(n) = 1$  and  $N(n) = n$  for every  $n \in \mathbb{N}$ . Equivalently, using Möbius inversion formula, the previous identity can be written as  $\varphi = \mu * N$  with  $\mu$  the Möbius function.

If we now define

$$S_k(n) := (U * \Phi_k)(n) = \sum_{d|n} \Phi_k(n),$$

we obtain again a multiplicative function whose values over prime-powers are given in the following result.

**Proposition 9.** *Let  $k$  be a positive integer. Then,*

$$\text{i) } S_k(2^r) = 1 + \varphi(2^k) \frac{2^{kr} - 1}{2^k - 1}.$$

ii) *If  $p$  is an odd prime:*

$$S_k(p^r) = \begin{cases} 1 + \varphi(p^k) \frac{p^{kr} - 1}{p^k - 1}, & \text{if } k \text{ is odd;} \\ 1 + \left( \varphi(p^k) - \varphi(p^{k/2}) \right) \frac{p^{kr} - 1}{p^k - 1}, & \text{if } k \text{ is even and } 4 \mid k \text{ or } 4 \mid p - 1; \\ 1 + \left( \varphi(p^k) + \varphi(p^{k/2}) \right) \frac{p^{kr} - 1}{p^k - 1}, & \text{if } k \text{ is even, } 4 \nmid k \text{ and } 4 \nmid p - 1. \end{cases}$$

*Proof.* It is a direct consequence of Proposition 4.  $\square$

Now, if  $\sigma$  is the usual divisor function, it is also known that  $S = U * \varphi = N = \mu * \sigma$ . This result can be generalized if  $k$  is odd in the following way (recall that  $\sigma_k(n) = \sum_{d|n} d^k$ ).

**Proposition 10.** *Let  $k$  be an odd integer. Then,*

$$S_k(n) = \sum_{d|n} \mu(d) d^{k-1} \sigma_k(n/d) = (n^{k-1} \mu * \sigma_k)(n)$$

*Proof.* First of all, observe that Corollary 1 implies that

$$S_k(n) = \sum_{d|n} \Phi_k(n) = \sum_{d|n} d^{k-1} \varphi(d) = \sum_{d|n} d^{k-1} \varphi(d) U(n/d).$$

Hence, we have that

$$\begin{aligned} S_k &= N^{k-1} \varphi * U = N^{k-1} (\mu * N) * U = (N^{k-1} \mu * N^k) * U = N^{k-1} \mu * (N^k * U) = \\ &= N^{k-1} \mu * \sigma_k, \end{aligned}$$

as claimed.  $\square$

**4.4. The average order of  $\Phi_k$ .** The average order of  $\varphi(n)$  is well-known [17]. Namely,

$$\sum_{n \leq x} \varphi(n) \approx \frac{3}{\pi^2} x^2.$$

In fact, the best known asymptotic formula is currently:

$$\sum_{n \leq x} \varphi(n) = \frac{3}{\pi^2} x^2 + \mathcal{O}(x(\log(x))^{2/3}(\log \log x)^{4/3}).$$

If  $k$  is odd we can give an easy generalization of this fact.

**Theorem 2.** *Let  $k \geq 1$  be an odd integer. Then*

$$\sum_{n \leq x} \Phi_k(n) = \frac{6}{\pi^2(k+1)} x^{k+1} + \mathcal{O}(x^k \log^{2/3} x (\log \log x)^{4/3})$$

*Proof.* For  $k = 1$  we have

$$\sum_{n \leq x} \varphi(n) = \frac{3}{\pi^2} x^2 + \mathcal{O}(x \log^{2/3} x (\log \log x)^{4/3}).$$

Let  $k > 1$  be an odd integer. As

$$\Phi_k(n) = n^{k-1} \varphi(n)$$

it is enough to apply the Abel's summation formula. Thus we obtain

$$\begin{aligned} \sum_{n \leq x} \Phi_k(n) &= \left[ \frac{3}{\pi^2} x^2 + \mathcal{O}(x \log^{2/3} x (\log \log x)^{4/3}) \right] x^{k-1} - \\ &\quad - (k-1) \int_1^x \left[ \frac{3}{\pi^2} t^2 + \mathcal{O}(x \log^{2/3} t (\log \log t)^{4/3}) \right] t^{k-2} dt \\ &= \frac{6}{\pi^2(k+1)} x^{k+1} + \mathcal{O}(x^k \log^{2/3} x (\log \log x)^{4/3}). \end{aligned}$$

$\square$



## 5. CONCLUSIONS AND FURTHER WORK

The generalization of  $\varphi$  that we have presented in this paper is possibly one of the closest to the original idea which consists of counting units in a ring. In addition, both the elementary and asymptotic properties of  $\Phi_k$  extend those of  $\varphi$  in a very natural way. There are many other results regarding  $\varphi$  that have not been considered here but that, nevertheless, may have their extension to  $\Phi_k$ . We now present some ideas in that direction.

**5.1. Dirichlet series for  $\Phi_k$ .** The Dirichlet series for  $\varphi(n)$  may be written in terms of the Riemann zeta function as:

$$\sum_{n=1}^{\infty} \frac{\varphi(n)}{n^s} = \frac{\zeta(s-1)}{\zeta(s)}.$$

Again, if  $k$  is odd, we easily get the following result.

**Proposition 11.** *Let  $k$  be an odd integer. Then,*

$$\sum_{n=1}^{\infty} \frac{\Phi_k(n)}{n^s} = \frac{\zeta(s-k)}{\zeta(s+1-k)}.$$

*Proof.* If  $k$  is odd recall that  $\Phi_k(n) = n^{k-1}\varphi(n)$ . □

**5.2. Menon's identity.** In 1965 P. Kesava Menon [12] proved the following identity:

$$\sum_{k|n; \gcd(k,n)=1} \gcd(k-1, n) = d(n)\varphi(n),$$

where  $d(n)$  denotes the number of divisors of  $n$ . This identity has been generalized in several ways [9, 10, 15]. Our work suggests the following generalization:

$$\sum_{\gcd(x_1^2 + \dots + x_k^2, n)=1} \gcd(x_1^2 + \dots + x_k^2 - 1, n) = \Gamma_k(n)\Phi_k(n),$$

where  $\Gamma_k(n)$  is a multiplicative function to be found.

## REFERENCES

- [1] Dorin Andrica and Mihai Piticari. On some extensions of Jordan's arithmetic functions. *Acta Univ. Apulensis Math. Inform.*, (7):13–22, 2004.
- [2] Leonard Eugene Dickson. *History of the theory of numbers. Vol. I: Divisibility and primality*. Chelsea Publishing Co., New York, 1966.
- [3] Leonard Eugene Dickson. *History of the theory of numbers. Vol. II: Diophantine analysis*. Chelsea Publishing Co., New York, 1966.
- [4] P. G. Garcia and Steve Ligh. A generalization of Euler's  $\varphi$ -function. *Fibonacci Quart.*, 21(1):26–28, 1983.
- [5] Miguel-C. Grau, J.M. and A.M. Oller-Marcén. On the structure of quaternion rings over  $\mathbb{Z}/n\mathbb{Z}$ . *arXiv:1402.0956 [math.RA]*, (1).
- [6] Oller-Marcén A.M. Rodríguez M. Grau, J.M. and D. Sadornil. Fermat test with gaussian base and gaussian pseudoprimes. *arXiv:1401.4708 [math.NT]*, (1).
- [7] P. Hall. The eulerian functions of a group. *Quarterly Journal of Mathematics*, os-7(1):134–151, 1936. Cited By (since 1996):98.
- [8] G. H. Hardy and E. M. Wright. *An introduction to the theory of numbers*. Oxford University Press, Oxford, sixth edition, 2008. Revised by D. R. Heath-Brown and J. H. Silverman, With a foreword by Andrew Wiles.
- [9] P. Haukkanen and J. Wang. A generalization of Menon's identity with respect to a set of polynomials. *Portugal. Math.*, 53(3):331–337, 1996.

- [10] Pentti Haukkanen. Menon's identity with respect to a generalized divisibility relation. *Aequationes Math.*, 70(3):240–246, 2005.
- [11] Jerzy Kaczorowski. On a generalization of the Euler totient function. *Monatsh. Math.*, 170(1):27–48, 2013.
- [12] P. Kesava Menon. On the sum  $\sum (a - 1, n)$ ,  $[(a, n) = 1]$ . *J. Indian Math. Soc. (N.S.)*, 29:155–163, 1965.
- [13] J. Sándor and B. Crstici. *Handbook of number theory. II*. Kluwer Academic Publishers, Dordrecht, 2004.
- [14] R. Sivaramakrishnan. The many facets of Euler's totient. II. Generalizations and analogues. *Nieuw Arch. Wisk. (4)*, 8(2):169–187, 1990.
- [15] Marius Tărnăuceanu. A generalization of Menon's identity. *J. Number Theory*, 132(11):2568–2573, 2012.
- [16] S. Thajoddin and S. Vangipuram. A note on Jordan's totient function. *Indian J. Pure Appl. Math.*, 19(12):1156–1161, 1988.
- [17] Arnold Walfisz. *Weylsche Exponentialsummen in der neueren Zahlentheorie*. Mathematische Forschungsberichte, XV. VEB Deutscher Verlag der Wissenschaften, Berlin, 1963.

DEPARTAMENTO DE MATEMÁTICAS, UNIVERSIDAD DEL PAÍS VASCO, FACULTAD DE CIENCIA Y TECNOLOGÍA, BARRIO SARRIENA, S/N, 44980 LEIOA, SPAIN  
*E-mail address:* `mtpcagac@lg.ehu.es`

DEPARTAMENTO DE MATEMÁTICAS, UNIVERSIDAD DE OVIEDO, AVDA. CALVO SOTELO, S/N, 33007 OVIEDO, SPAIN  
*E-mail address:* `grau@uniovi.es`

CENTRO UNIVERSITARIO DE LA DEFENSA, CTRA. DE HUESCA, S/N, 50090 ZARAGOZA, SPAIN  
*E-mail address:* `oller@unizar.es`